From: Ali Lange <arlange@google.com>
Sent: Thursday, October 24, 2019 3:35 PM
To: privacyframework <privacyframework@nist.gov>
Cc: Lawrence You <lyou@google.com>
Subject: Google Comments on NIST Framework

Please see attached. Email arlange@google.com with questions. Thank you!

--

Ali Lange | Public Policy | arlange@google.com | 415-736-4643

Google

National Institute of Standards and Technology
100 Bureau Drive
Stop 2000
Gaithersburg, MD 20899

October 24, 2019

Re: NIST Privacy Framework: Preliminary Draft Comments

Google appreciates the opportunity to provide comments in response to the National Institute of Standards and Technology (NIST) Request for Comment on "NIST Privacy Framework: Preliminary Draft."[1] Google recognizes the longstanding leadership of the US Commerce Department in promoting data privacy policies that enable continued innovation and, we appreciate the Department's open and consultative processes for developing policy and technical frameworks including this Privacy Framework. We also appreciate that there will be further opportunities to refine the Privacy Framework after this draft is finalized, and applaud your commitment to maintaining this material as an evergreen resource.

We recognize the challenge NIST accepted in producing the Privacy Framework to complement their Cybersecurity Framework.[2] While the objectives of cybersecurity are more clear, privacy is personal and the risks vary not only among individuals and cultures but also depend on the purpose for which personal information is collected and used. While policymakers debate a baseline privacy law in the U.S. (something Google has supported),[3] data protection is an essential and increasing part of everyday business operations. Organizations are looking for guidance on how to meet expectations.

The broad interest in appropriate privacy procedures is responsive to the enactment of data protection regulation around the world, but perhaps more importantly it is a signal that companies have a business interest in establishing a strong reputation on data protection. At Google we understand that the promise of our technology, and the success of our business, hinges upon our ability to earn and maintain a strong reputation built on the trust of our users. The methodology presented in NIST's Framework echoes some of the key insights that we have gained in over 20 years of building products and features that have provided increasingly higher utility, and incumbent management of, personal information.

We share the following observations to support NIST as it prepares to publish the first draft of the Framework. In this comment, we highlight our broad agreement with the approach and

[1] Preliminary Draft of the NIST Privacy Framework, 84 Fed. Reg. 47255 (Sept. 9, 2019).
[2] NIST Cybersecurity Framework, https://www.nist.gov/cyberframework
[3] In comments to the Department of Commerce [Docket No. 101214614-0614-01 and Docket No. 1004] in 2010, Google called for the passage of comprehensive baseline privacy legislation. We reiterated this view in our comments to the Department of Commerce [Docket No. 180821780-8780-01] in 2019.

recommendations and indicate topics where we think additional details in future iterations would be beneficial. We are eager to see your final product used by organizations from all sectors, and believe that adopting this Framework can lead to better outcomes for individuals in many facets of their daily life.

Taking a Risk-Based Approach

We support and agree with NIST's recommendation that organizations utilize a risk-based methodology while developing, operating and maintaining their privacy programs. The diversity of contexts around processing personal information is incalculable, and individual privacy risks can change based on the situation and over time as technology products and individual expectations evolve. The organizing concepts in the Privacy Framework provide a useful functional categorization and dovetails with the Cybersecurity Framework, allowing practitioners who span privacy and security domains to reuse common knowledge. It presents risks within organizations and key stakeholders in a conceptually similar manner, with efficiency.

The design of an internal privacy program can be complex and difficult to summarize, but the objective of any program must be to mitigate or otherwise address the risks of adverse uses of personal information. Google's privacy program includes hundreds of employees who are focused on privacy full-time, in addition to a privacy training program that is required of every employee up to and including our executives and a design and review process that touches every product we launch. Moreover, more than half of our employees, including software engineers and product managers, are enrolled in a special in-depth training shortly after they join the company, and we also provide topic-specific training on security and privacy.

Google's privacy program maps well to the Framework and includes governance through policies and process, privacy design consultation and reviews, engineers dedicated to privacy to review code and data flows, common infrastructure we build to support privacy features and data management, and a system to manage and address any issues discovered before products are launched. Google has had a comprehensive data protection program for over seven years, and we continue to expand and refine it.[4] Moreover, our privacy program complements and is operated in conjunction with the information security teams, products, and processes. We are proud of our privacy program, and at the same time we recognize that each organization must develop a program that corresponds to its own needs and risk. NIST's Framework provides an instruction manual for the analysis needed to do just that.

Our consumer products have evolved to increase transparency (communication) on the information they use, and to give users choices and control over that information. Further, we provide many methods of communicating data processing practices to many constituents

[4] Written Testimony of Keith Enright, Chief Privacy Officer, Google, United States Senate Committee on Commerce, Science, and Transportation Hearing on "Examining Safeguards for Consumer Data Privacy." Sept 26, 2018. www.commerce.senate.gov/services/files/5D32673E-D11D-4EE1-A7F3-8B03E407128D

including business partners such as customers across advertising, enterprise applications, and cloud businesses; certifying and regulatory agencies, as well as the general public.

Supporting Privacy Across Sectors

We agree with the objective for the Privacy Framework to support organizations across sectors and business models. Managing personal information plays a role in the day-to-day operation of organizations of all sizes and types, including government agencies, universities, non-profits, and political campaigns as well as private industry. The Privacy Framework does not overlook the diversity of use cases, but instead accommodates an iterative and customizable approach based on the risks an organization has identified. This approach will work well for Google as its business grows in size and diversity, and we would apply the Framework as appropriate to various sub-organizations and businesses, whether for consumer productivity products, entertainment, mobile/desktop/IoT devices and services.

NIST is not alone in identifying the broad utility for privacy guidance. The necessity for organizations of all types to establish a methodology for privacy decisions is implicitly acknowledged in the scope of the General Data Protection Regulation (GDPR), which governs the processing of personal information across sectors in the European Union (EU). Additionally, organizations outside of the technology industry (and in particular those that are located outside the EU and do not have features directed to European users) might find the most value in NIST's Framework as they may not have already reviewed their practices.

Additionally, we praise the Framework's applicability to organizations that are seeking to update an existing privacy program, as well as for those establishing one. This aligns with Google's observation that our work on privacy is never complete, but always iterating. As NIST acknowledged in the Framework, regulation can direct the nature of changes to an organization's privacy program. For example, we estimate that Google invested hundreds of human-years of engineering, legal, and other work preparing for the General Data Protection Regulation (GDPR). This process was managed through our robust privacy program (described above), and it spurred improvements and further investments in our program. The results go beyond improved compliance, and might be best represented by some of our recently launched, industry-leading features like auto-delete for activity data[5] and other changes that make it easier for individuals to make privacy decisions that work for them.[6]

Establishing a Shared Vocabulary

In addition to supporting risk reduction for individuals, the Privacy Framework responds to business's need for shared vocabulary and common benchmarks for privacy communications.

---

[5] Monses, D and Marlo, M. "Introducing auto-delete controls for your Location History and activity data." https://www.blog.google/technology/safety-security/automatically-delete-data/ May 1, 2019.

[6] Miraglia, E. "Privacy that works for everyone" https://www.blog.google/technology/safety-security/privacy-everyone-io/ May 7, 2019. "Keeping privacy and security simple, for you" https://www.blog.google/technology/safety-security/keeping-privacy-and-security-simple-you/ Oct 2, 2019.

When organizations work collaboratively with data, agreement on the privacy protocols for the work improves the outcomes (whether or not there is a commercial relationship between the organizations). However, this can be challenging if the organizations are using different internal methodologies to manage privacy risk.

For example, a shared vocabulary around privacy helps cloud service providers (CSP) and customers understand how data is collected and used when delivering cloud services. In some cases, there is broad regulatory guidance on the division of responsibilities, but in any case a shared vocabulary and understanding of a fundamental processes results in consistent and clear communications about privacy risks and mitigations. Typically, the customer controls and administers the use of cloud services, including privacy-related settings. A shared vocabulary around a privacy policy or notice helps both CSPs and businesses understand the roles, responsibilities, and operational management processes related to privacy.

Additionally, government officials around the world are seeking a better understanding of how privacy decisions are managed within organizations (including government agencies). Whether or not a particular agency uses the Framework itself, NIST's description of a baseline methodology for assessing and mitigating privacy risks provides helpful information to global stakeholders on techniques used to manage privacy risk.

Privacy as a Multi-Disciplinary Concept

We were encouraged to participate through the Framework drafting process in discussions with experts spanning legal, compliance, privacy, and security engineering (among others). The nature of privacy and managing risk within organizations crosses these boundaries, and more often today we rely on privacy leaders and practitioners who are often jointly evaluating human factors in communication/presentation, the language of policy or regulation or the language of machine readable programs/data. The Framework supports this work by providing organizing subcategories that may be addressed by different parts of an organization, and then expressed and communicated to a diverse stakeholder group. We expect the Framework's breadth to be useful in a large cross-organizational privacy program like ours.

Collaborating on Informative References

As mentioned above, one of the most valuable promises of the Privacy Framework is NIST's commitment to maintain its relevance with revisions and a refreshed supply of Informative References. Principles, best practices, and research are all essential components of keeping any privacy program aligned with the latest understanding of risk and expectations.

In addition to analytical guidance, NIST should include technical and practical tools among their Informative References. Google is committed to sharing technical details of our privacy work with the open source and academic research communities whenever possible. We invest considerable resources into developing cutting-edge engineering techniques that help us

protect the privacy and security of our users' data. And we make much of our research available to open-sources communities so that everyone can benefit from these privacy-preserving protocols. For example, we have recently published several open source libraries directly relevant to the Privacy Framework, including:

- **Differential Privacy:** This area of technology enables organizations to gain useful insights while reducing data processing risks to better preserve individuals' privacy.[7]
- **TensorFlow Federated (TFF):** TFF is an open source framework for experimenting with machine learning and other computations on decentralized data.[8]
- **Private Join and Compute:** This protocol enables people to compute statistics about the intersection of two sets of data without revealing personally identifiable information.[9]
- **Data Transfer Project:** The DTP will make it easier for people to control their personal information by moving it to and from different services.[10]

We also continue to publish our research findings in peer-reviewed academic conferences and journals to provide visibility into our findings to the entire privacy community.[11] We look forward to continuing to share resources like this, and others, with NIST as part of their library of Informative References.

Future iterations

As with the Cybersecurity Framework, we appreciate NIST's commitment to continuing to iterate on this resource to incorporate learnings and new information. Specifically, we expect that a few of the topics raised in this draft are likely to see future revisions or additional nuance.

---

[7] Guevara, M. "Enabling developers and organizations to use differential privacy" https://developers.googleblog.com/2019/09/enabling-developers-and-organizations.html. September 5, 2019.

[8] Ingerman, A. and Ostrowski, K. "Introducing TensorFlow Federated" https://medium.com/tensorflow/introducing-tensorflow-federated-a4147aa20041 March 6, 2019.

[9] Walker, A. Patel, S. and Yung, M. "Helping organizations do more without collecting more data" security.googleblog.com/2019/06/helping-organizations-do-more-without-collecting-more-data.html. June 19, 2019.

[10] Data Transfer Project https://datatransferproject.dev/ Accessed October 22, 2019.

[11] A few recent publications:
Thomas, K., et al. "Protecting accounts from credential stuffing with password breach alerting" https://www.usenix.org/conference/usenixsecurity19/presentation/thomas.
Sambasivan, N., et al. ""They Don't Leave Us Alone Anywhere We Go": Gender and Digital Abuse in South Asia" https://dl.acm.org/citation.cfm?id=3300232.
Sleeper, M., et al. "Tough Times at Transitional Homeless Shelters: Considering the Impact of Financial Insecurity on Digital Security and Privacy" https://dl.acm.org/citation.cfm?id=3300319.
Desfontaines, D., et al. "Cardinality Estimators do not Preserve Privacy" https://arxiv.org/abs/1808.05879.
Peddinti, S., et al. "Reducing Permission Requests in Mobile Apps" https://dl.acm.org/citation.cfm?id=3355584.

First, we anticipate that future iterations of the Privacy Framework will include additional discussion and information on the variables that contribute to variance in individual privacy risk. As we noted in our comments on an earlier draft of this Framework, factors like the type of processing, the stakes of the result, and the individual's specific circumstances or tolerance can motivate their assessment of the privacy risk of engaging with any organization.[12] The draft currently acknowledges the need to consider individual risk, but provides minimal guidance on how to balance the preferences among individuals in developing privacy program. Providing more detailed guidance on this topic would be a valuable addition to the Framework.

Second, organizations who leverage the Privacy Framework might find it helpful to have a more detailed definition of symptoms of the privacy problems described in the Framework. Describing what system components should be monitored to detect such problems will help organizations develop a methodology to prioritize their resources. As will connecting the problems to concrete illustrations of the types of adverse outcomes organizations should be aiming to avoid.

Third, as many sectors continue to expand on the access, use, transfer, and sharing of personal information, it may be helpful for the Framework to address a growing need for multi-party risk assessment and management. More businesses' products and services, government organizations, and institutions today rely on authenticated access to individuals' accounts, whether via API, URL/HTTP request, or app permission. If the history of the Cybersecurity Framework is an indicator, we hope to see modifications to the Privacy Framework, as well as standards, frameworks, tools, and services that will facilitate risk management across organizations.

Finally, the next iteration of the Privacy Framework might include additional advice for complex organizations that may share overarching goals and top-level risk management, but may need to specify multiple but compatible profiles. Once the vocabulary and practice of the Framework advances, we would welcome seeing examples or best practices that may be useful to evolving and growing organizations.

Conclusion

The foundation of Google's business is the trust of people that use our services. To maintain and foster this trust, we clearly explain how our products use personal information and provide controls to help our users manage their privacy. We also invest in research and development of cutting-edge privacy and security engineering techniques, sharing what we learn to benefit the broader data ecosystem.

[12] Kissner, Lea, Comment on Developing a Privacy Framework (January 14, 2019) https://www.nist.gov/sites/default/files/documents/2019/02/04/google_lea_kissner_508.pdf.

Through this work, we've learned a great deal about building a robust and maturing privacy program, and about how to optimize for strong transparency, choice, and control by empowering users with best in class settings and controls. NIST's work will inform our continued efforts, and we are optimistic about the impact of NIST's work to enable similarly robust programs across industries and geographies. We look forward to continuing to work with NIST as the Privacy Framework is finalized and shared with the world.

Respectfully submitted,

Lawrence You
Director of Privacy, Product and Engineering
Google

Ali Lange
Global Affairs and Public Policy Manager
Google